No. 17-2

In the Supreme Court of the United States

UNITED STATES OF AMERICA,

Petitioner,

v.

MICROSOFT CORPORATION,

Respondent.

On Writ of Certiorari to the United States Court of Appeals for the Second Circuit

BRIEF OF INTERNATIONAL AND EXTRATERRITORIAL LAW SCHOLARS AS AMICI CURIAE IN SUPPORT OF RESPONDENT

Anthony Colangelo
SMU DEDMAN SCHOOL OF LAW
3315 Daniel Ave.
Dallas, Texas 75205
(214) 768-2372

Austen Parrish
INDIANA UNIVERSITY MAURER SCHOOL OF LAW
211 S. Indiana Ave.
Bloomington, Indiana 47405
(812) 855-8885

J. Carl Cecere
Counsel of Record
CECERE PC
6035 McCommas Blvd.
Dallas, Texas 75206
(469) 600-9455
ccecere@cecerepc.com

TABLE OF CONTENTS

Table of Contents i
Table of Authorities iii
Interest of Amici Curiae 1
Summary of the Argument 1
Argument 5
I. The SCA does not authorize law-enforcement officers to violate international law by seizing electronic data physically stored in another country. 5
A. International law prohibits unilateral execution of a warrant inside another country's sovereign territory. 6
B. Under the *Charming Betsy* canon, the SCA's silence on these violations of international law means Congress has not authorized them. 10
C. The Government's position is irreconcilable with our international legal obligations and *Charming Betsy*. 11
1. No international treaty permits unilateral trans-state seizure of private electronic data. 12
2. The Government's analogy to civil subpoenas fails. 19
II. Transnational seizures of private electronic data also exceed the SCA's territorial boundaries 23

TABLE OF CONTENTS—continued

A. The Government's effort to sanction the unilateral seizure of private emails of foreign citizens stored abroad impermissibly narrows the focus inquiry. 24

B. The principles that drive extraterritoriality analysis support this broad reading of Section 2703's focus. 28

1. The Government's approach invites clashes with foreign nations without congressional authorization. 29

2. The Government's approach undermines the separation of powers and shared assumptions about Congress's approach to lawmaking. 31

C. The Government's concerns about protecting law-enforcement efficacy are best addressed to Congress 34

Conclusion 36

Appendix i

TABLE OF AUTHORITIES

Cases

Benz v. *Compania Naviera Hidalgo*,
353 U.S. 138 (1957) 10

EEOC v. *Arabian Am. Oil Co. (Aramco)*,
499 U.S. 246 (1991) 10, 27, 31

F. Hoffman-La Roche Ltd. v. *Empagran S.A.*,
542 U.S. 155 (2004) 10

FTC v. *Compagnie de Saint-Gobain-Pont-A-Mousson*,
636 F2d 1300 (D.C. Cir. 1980) 8

George Pinson (Fr.) v. *United Mexican States*,
5 R.I.A.A. 327 (422 Perm. Ct. Arb. 1928) 13

Graco, Inc. v. *Kremlin, Inc.*,
101 F.R.D. 503 (N.D. Ill. 1984) 21

Hartford Fire Ins. Co. v. *California*,
509 U.S. 764 (1993) 10, 11, 19, 20

Japan Line, Ltd. v. *Cty. of Los Angeles*,
441 U.S. 434 (1979) 32

Kiobel v. *Royal Dutch Petrol. Co.*,
569 U.S. 108 (2013) 27, 28, 29, 30, 33

Loucks v. *Standard Oil Co. of New York*,
224 N.Y. 99 (1918). 20

McCulloch v. *Sociedad Nacional de Marineros de Honduras*,
372 U.S. 10 (1963) 10, 11

McKenna v. *Fisk*,
12 U.S. 241 (1843) 6

Morrison v. *Nat'l Australia Bank*,
561 U.S. 247 (2010) ..... passim

Cases—continued

Murray v. *The Schooner Charming Betsy*,
6 U.S. (2 Cranch) 64 (1804) ..... passim

PCIJ, SS Lotus (France v *Turkey)*,
PCIJ Reports, Series A, No. 10 (1927) 6

Rafael v. *Verelst*,
1058 2 W. Bl. (1055) 7

RJR Nabisco, Inc. v. *European Cmty.*,
136 S. Ct. 2080 (2016) 6, 23, 26, 29

The Schooner Exch. v. *McFaddon*,
11 U.S. 116 (1812) 6

Skinner v. *Ry. Labor Executives' Ass'n*,
489 U.S. 602 (1989) 8

Sosa v. *Alvarez–Machain*,
542 U.S. 692 (2004) 27, 30, 31

In re Terrorist Bombings of U.S. Embassies in E. Africa,
552 F.3d 157 (2d Cir. 2008) 7

United States v. *Verdugo-Urquidez*,
494 U.S. 247 (1990) 7

Statutes and Legislative Materials

Alien Tort Statute,
28 U.S.C. § 1350, *et seq.*. 27
28 U.S.C. § 1350. 27

Foreign Evidence Request Efficiency Act,
18 U.S.C. § 3512 *et seq* 7
§ 3512 (a)(1) 7
§ 3512 (a)(2)(B) 7

Statutes and Legislative Materials—continued

Stored Communications Act,
Pub. L. No. 99-508, tit. II, 100 Stat. 1860 (Oct. 21, 1986) (18 U.S.C. § 2701 *et seq.*) 2, 17
§ 2702 7
§ 2703 ..... passim
§ 2703(a) 7, 26
§ 2703(g) 7
§ 2711(4) 7, 32
H.R. Rep. No. 99-647 (1986) 24, 26
Law Enforcement Access to Data Stored Across Borders: Hearing Before the S. Subcomm. on Crime and Terrorism (May 24, 2017), <goo.gl/T7Ai7u> 30

Foreign Statutes and Regulations

French Penal Code Law No. 80-538 21
Commission Regulation 2016/679, 2016 O.J. (L 119) 64 21

Treaties

Council of Europe Convention on Cybercrime Nov. 23, 2001, S. Treaty Doc. No. 11, 108th Cong., 1st Sess. (2003) 2296 U.S. U.N.T.S. 167 12
art. 18 ..... 14, 16, 18
art. 18.1 16
art. 18.1(a), ... 12, 13, 15, 16
art. 18.1(b) 15
art. 18.3 15
art. 19 18

Treaties—continued
art. 32 ..... 13, 14, 18
Vienna Convention on the Law of Treaties, May 23, 1969, 1155 U.N.T.S. 331 13
art. 31.3(c) 13

Other Authorities

Gary B. Born & Peter B. Rutledge, *International Civil Litigation in U.S. Courts* (5th ed. 2011) 21
Anthony J. Colangelo, *Absolute Conflicts of Law*, 91 Ind. L. J. 719 (2016) 30
Convention on Cybercrime, Explanatory Report (Nov. 23, 2001) 14, 16
Cybercrime Convention Committee, Council of Europe, T-CY Guidance Note #10 .....14, 15, 16, 17
Robert Cryer et al., *An Introduction to International Criminal Law and Procedure* (2d ed. 2010) 6
Jennifer Daskal, *The Un-Territoriality of Data*, 125 Yale L.J. 326 (2015) 7
États-Unis – Union européenne - Q&R - Extrait du point de presse (Jan. 4, 2018), <https://goo.gl/ferJG8> 21
International Law Association, *Report of the Fifty-First Conference* (1964) 19
Mann, *The Doctrine of Jurisdiction in International Law*, 1 Rec. Des Cours 1 (1964) 8
Baron Arnold Duncan McNair, *The Law of Treaties* (2d ed. 1961) 13

Other Authorities—continued

National Commission of Reform of Federal Criminal Laws, *Final Report* (1971) 24

Office of Legal Education Executive Office for United States Attorneys, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (2009) (DOJ Manual) 9

Joost Pauwelyn, *The Rule of Public International Law in the WTO: How Far Can We Go?*, 95 Am. J. Int'l L. 535 (2001) 13

Tonya Putnam, Courts Without Borders (2016) 31

Restatement (Third) of the Foreign Relations Law of the United States (1987) 6, 20

Joseph Story, *Commentaries on the Conflict of Laws* (1834) 20

United Nations General Assembly, Resolution 56/83, Annex, art. 5, *Responsibility of States for Internationally Wrongful Acts* (2001) 8

United Nations, General Assembly, Resolution 2625 (XXV), annex, *Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations* (Oct. 24, 1970) 19, 20

INTEREST OF AMICI CURIAE[1]

Amici are law professors with expertise in international, extraterritorial, and privacy law. We share an interest in the proper understanding of the *Charming Betsy* canon of construction and the law of extraterritoriality. We submit this brief to clarify how these doctrines should be applied in this case, and to explain how each independently bars interpreting the Stored Communications Act (SCA) to allow seizure of electronic data from inside Ireland's sovereign territory. We also wish to highlight certain flaws in the analysis the Government offers in this case, which fails to account for *Charming Betsy*, and espouses too narrow a view of the SCA's focus, in its effort to escape the Act's acknowledged territorial boundaries and authorize plainly extraterritorial conduct.

Biographical information for each signatory to this brief is provided in the appendix.

SUMMARY OF THE ARGUMENT

Both the *Charming Betsy* canon and the law of extraterritoriality fit within a well-defined body of law this Court has developed for determining how American law applies abroad. These doctrines exist independently: one aims to avoid unsanctioned violations of international law. The other prevents the improper projection of

---

[1] Petitioner and respondent have both lodged blanket amicus consent letters with the Court. No counsel for any party authored this brief in whole or in part, and no entity other than amici or their counsel made a monetary contribution to the preparation or submission of this brief.

American legal power beyond our borders. But they share much in common. Both rest on a properly restrained understanding of the judiciary's proper place in our constitutional order, under which the often-delicate issues of foreign affairs in lawmaking are properly reserved to Congress, not courts. And both are grounded on shared insights the Court has gained over time about Congress's approach to lawmaking: Its preference for "domestic, not foreign matters," *Morrison* v. *Nat'l Australia Bank*, 561 U.S. 247, 254 (2010); its respect for other nations' sovereignty; its regard for international law; its inclination toward international collaboration; and perhaps most importantly of all, its avoidance of international friction and strife—unless some overriding policy need compels congressional action despite the risk of such strife.

Yet the Government urges a departure from both the letter and spirit of these doctrines in its interpretation of the Stored Communications Act (SCA), 18 U.S.C. § 2701 *et seq*. The Government claims the SCA's warrant provision conveys to it the power to seize private email communications, likely belonging to Irish citizens, housed in an Irish data center, without Ireland's consent or cooperation. And the Government contends that it shares this international seizure power with state and local law enforcement officials. This based on a statute the Government admits has no extraterritorial reach, utilizing electronic storage and retrieval mechanisms that Congress could hardly have *conceived* of, let alone authorized, when the SCA was enacted.

The Government claims this is possible because, in its view, these electronic incursions into foreign sovereign territory simply do not count in the extraterritoriality

analysis. As the Government sees it, the focus of the Act's warrant provision is limited to the "disclosure" that occurs when Microsoft employees retrieve the data from a computer terminal at Microsoft's corporate headquarters in Redmond, Washington, and turn it over to law enforcement. Gov't Br. 21–23. But this position cannot be squared with the doctrines developed in the Court's precedents.

The first problem with the Government's theory is that—irrespective of the SCA's extraterritorial reach—the electronic seizure of electronic records physically located in another country is an exercise of extraterritorial enforcement jurisdiction. That is a plain violation of international law, no different than if FBI agents set foot on Irish soil to retrieve the data themselves. Under the *Charming Betsy* canon, first enumerated by Chief Justice Marshall in *Murray* v. *The Schooner Charming Betsy*, U.S. courts are constrained to avoid interpreting "an act of congress" in a manner that would "violate the law of nations, if any other possible construction remains," 6 U.S. (2 Cranch) 64, 118 (1804)—whether the statute at issue is meant to apply extraterritorially or not. Congress gave no hint in the SCA that it intended for warrants under Section 2703 to authorize violations of international law, and the Government provides no reason to believe these violations can be ignored. Application of the *Charming Betsy* canon thus requires finding that the Government's requested power to seize electronic records from Ireland exceeds the authority conveyed under the SCA.

The Government's theory also has problems under the law of extraterritoriality itself. Even if the ambit of Section 2703's focus were limited to "disclosure"—a point

that Microsoft persuasively rebuts—that focus would still incorporate the use of Section 2703 warrants to compel electronic retrieval of data located in other countries. Section 2703's text may speak only of "disclosure," but the power it conveys extends beyond the page, authorizing law-enforcement officials to compel providers to perform an entire sequence of steps needed to effectuate disclosure. That whole range of authorized conduct necessarily lies within the Act's focus, and was the subject of Congress's legitimate concern in crafting it. Accordingly, if law-enforcement officials wish to use Section 2703 warrants to compel disclosure of emails stored in other countries, they need express authorization from Congress to do so, which all agree Congress has not provided. The correct result then is to reject the Government's position in this case.

That result is also necessary to remain faithful to this Court's precedents and the principles behind its extraterritoriality doctrine. The U.S.'s aggressive stance on compelled disclosure of information stored abroad has already created pronounced friction with other countries. A Government win here would further stoke those resentments—and could realistically provoke retaliation—at a time when Congress has indicated a preference for détente and international cooperation through treaties. Much remains to be developed in this area of the law to promote legitimate law enforcement needs, to address our sovereign neighbors' security concerns, and to protect our citizens' liberty and security. But only Congress is properly equipped to deal with these sensitive issues. That prerogative should not be handed over to judges or federal law enforcement—and certainly should not be enjoyed by the state and local law enforcement officials

who are also empowered to use the SCA's warrant provisions.

Rejecting the Government's position is likewise essential to preserve assumptions about extraterritoriality that the legislative and judicial branches have shared since the Republic's early days. These shared assumptions properly constrain law enforcement and other governmental actors. They also prevent the march of technological progress from introducing an extraterritorial creep into laws that Congress intended to remain domestically fixed.

This is not to say that U.S. enforcement powers should never reach into a foreign country. It may be that borderless law enforcement is necessary for combatting terrorism or certain types of transnational crimes. There may be situations when no international treaty exists, where bilateral cooperation is impossible, or where remote cross-border searches are necessary to prevent criminal evasion. But none of those circumstances exist here. And even if they did, a proper regard for the separation of powers—and the branches' respective institutional competences—demands that Congress be the one to make those calls.

ARGUMENT

I. The SCA does not authorize law-enforcement officers to violate international law by seizing electronic data physically stored in another country.

Because the Government agrees that the SCA permits no extraterritorial application, the Government's case begins and ends with an examination of Section 2703's "focus," the "second step" required in an extrater-

ritoriality analysis. Gov't Br. 17; see also *RJR Nabisco, Inc.* v. *European Cmty.*, 136 S. Ct. 2090, 2100 (2016). Yet there is another canon of statutory construction that the Government entirely neglects—and that resolves this case: the *Charming Betsy* canon, which imposes independent limits on Section 2703's reach. That canon prohibits interpreting U.S. statutes in a manner that would violate international law unless Congress has authorized the violation in the statute itself. And just such an unsanctioned international-law violation would occur if law-enforcement officers used Section 2703 warrants to seize data physically stored in other countries.

A. International law prohibits unilateral execution of a warrant inside another country's sovereign territory.

Because a country's authority within its boundaries is "exclusive and absolute," *The Schooner Exchange* v. *McFaddon*, 11 U.S. 116, 136 (1812), "[t]he first and foremost restriction imposed by international law on a State is *** [that] it may not exercise its power in any form in the territory of another State." *PCIJ, SS Lotus (France v Turkey)*, PCIJ Reports, Series A, No. 10, p. 19 (1927). This restriction walls-in law-enforcement officials, prohibiting them from "exercise[ing] their functions in the territory of another state" without "the consent of the other state." *Restatement (Third) of the Foreign Relations Law of the United States* § 432; *id.* cmt. b. B. Law enforcement is an exercise of "enforcement jurisdiction"—the "most intrusive of jurisdictional claims." Robert Cryer et al., *An Introduction to International Criminal Law and Procedure* 44 (2d ed. 2010). And going back to the Founding, it has been considered a fundamentally local activity. *McKenna* v. *Fisk*, 12 U.S. 241, 248

(1843) ("'Crimes are in their nature, local, the jurisdiction of crimes is local,'" quoting *Rafael* v. *Verelst*, 1058 2 W. Bl. (1055)).

Execution of a warrant in another country without its consent is a paradigmatic exercise of enforcement jurisdiction, and a plain violation of international law. *In re Terrorist Bombings of U.S. Embassies in E. Africa*, 552 F3d 157, 171 (2d Cir. 2008) (noting that warrants lack extraterritorial reach); see also Jennifer Daskal, *The Un-Territoriality of Data*, 125 Yale L.J. 326, 354 (2015) ("The overarching rule is that the judiciary's warrant authority is territorially limited.") (citing authorities).

This Court has recognized this territorial limit on warrant enforcement in its constitutional jurisprudence. See *United States* v. *Verdugo-Urquidez*, 494 U.S. 259, 279 (1990) (noting that a "warrant" is a "dead letter outside of the United States"). And Congress likewise observes this limit in lawmaking—as the SCA itself demonstrates. The SCA prohibits foreign governments from enforcing *their own* warrants to obtain data in the United States, through its refusal to list turnover to foreign governments among the disclosures permitted under Section 2702. It likewise bans foreign governments from obtaining a warrant in *this country* to obtain data located here. The SCA excludes foreign governments from the list of "governmental entities" entitled to apply for a Section 2703 warrant. And that ban is subject to only one narrow exception—provided in the Foreign Evidence Request Efficiency Act, 18 U.S.C. § 3512 *et seq.*—which still offers no direct route to obtaining a U.S. warrant. It instead requires that he foreign government ask the Department of Justice to obtain a Section 2703 warrant on its behalf, 18 U.S.C. § 3512 (a)(1) & (a)(2)(B), ensuring

that any foreign law-enforcement operations conducted in this country will be subject to strict Department supervision.

The Government cannot sidestep these universally recognized dictates of international law simply by conscripting Microsoft to conduct the retrieval on its behalf. Where a private party conducts a seizure "by compulsion of sovereign authority," that seizure is "attributable to the Government." *Skinner* v. *Ry. Labor Executives' Ass'n*, 489 U.S. 602, 614–615 (1989); see also United Nations General Assembly, Resolution 56/83, Annex, art. 5, *Responsibility of States for Internationally Wrongful Acts* (2001) ("The conduct of a person or entity which is not an organ of the State *** but is empowered by law *** to exercise elements of the governmental authority shall be considered an act of the State under international law.").

The fact that retrieval would be initiated electronically from inside the United States, at Microsoft's Redmond, Washington corporate headquarters, without travel to Ireland, also does not change the seizure's fundamentally international character. Such remote electronic retrieval efforts would still be "directed towards consummation, and require compliance" in Ireland, even if they were "initiated" in the U.S., and thus raise the same "problem of enforcement jurisdiction" as "when a State acts in foreign territory itself." *FTC* v. *Compagnie de Saint-Gobain-Pont-A-Mousson*, 636 F.2d 1300, 1316 n.89 (D.C. Cir. 1980) (quoting Mann, *The Doctrine of Jurisdiction in International Law*, 1 Rec. Des Cours 1, 128 (1964)). At bottom, using a computer in Washington to retrieve emails from Ireland is a projection of American enforcement power abroad—one reaching physically into

the sovereign territory of another country to seize private property, the same as when foreign countries like Russia illicitly access American computer networks from outside the United States to steal our citizens' personal information.

Indeed, the Government's dismissal of data's physical location as a peripheral concern in seizures is a departure from its own established position. In the Department of Justice's manual on computer searches and electronic surveillance, the Department almost seems to channel Microsoft when it advises that the location "where the remotely stored data is located" is the *key* consideration for determining the proper means to access it lawfully. Office of Legal Education Executive Office for United States Attorneys, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 84 (2009) (DOJ Manual). The DOJ Manual cautions that when the data is stored outside the United States, "the United States may be required to take actions ranging from informal notice to a formal request for assistance to the country concerned," *id.* at 85, usually using methods provided under the sorts of mutual legal assistance treaties (MLATs)—like the one the U.S. has with Ireland—that Government now derides as ineffectual, antiquated, and irrelevant, Gov't Br. 44–45. The DOJ Manual elsewhere explains the need for this cautious, consent-based approach, explaining that "in general, law enforcement officers exercise their functions in the territory of another country only with the consent of that country," so unilateral action would be improper. DOJ Manual 56–57. The Department itself thus agrees that non-consensual searches of data located in another country are a violation of international law.

B. Under the *Charming Betsy* canon, the SCA's silence on these violations of international law means Congress has not authorized them.

These principles of international law are not inviolate. Congress "clearly has constitutional authority" to exceed these "customary international-law limits," *Hartford Fire Insurance Co.* v. *California*, 509 U.S. 764, 815 (1993) (Scalia, J., dissenting), and sanction international exercises of enforcement jurisdiction—if it so desires. But the Court operates on the principle that "legislators take account of the legitimate sovereign interests of other nations when they write American laws," and thus "ordinarily seek[] to follow" these "principles of customary international law," *F. Hoffman-La Roche Ltd.* v. *Empagran S.A.*, 542 U.S. 155, 164 (2004). The Court therefore follows the prudent course, first charted in *Charming Betsy*, that courts should look for some "'affirmative intention of the Congress clearly expressed'" before allowing violations of international law. *McCulloch* v. *Sociedad Nacional de Marineros de Honduras*, 372 U.S. 10, 21–22 (1963) (quoting *Benz* v. *Compania Naviera Hidalgo*, 353 U.S. 138, 147 (1957)). The Court also construes ambiguous statutes "to avoid unreasonable interference with the sovereign authority of other nations." *Empagran*, 542 U.S. at 164.

Charming Betsy's "practice of using international law to limit the extraterritorial reach of statutes is firmly established in our jurisprudence," *Hartford Fire*, 509 U.S. at 817 (Scalia, J., dissenting). And it is "'wholly independent' of the presumption against extraterritoriality," *id.* at 815 (quoting *EEOC* v. *Arabian American Oil Co.* (*Aramco*), 499 U.S. 246, 264 (1991), applying even "if

the presumption against extraterritoriality has been overcome or is otherwise inapplicable, *id.* at 814.

Like the presumption against extraterritoriality, the *Charming Betsy* canon is fundamentally about preserving the proper balance of judicial and legislative functions. Courts have no place entering the "'delicate field of international relations" absent Congress's express permission. *McCulloch*, 372 U.S. at 21–22 (quoting *Benz*, 353 U.S. at 147).

Nothing in Section 2703—or anywhere else in the SCA—provides the clear expression of congressional will required to permit violations of international law. That can only mean Congress has not authorized them. Accordingly, regardless of the SCA's "focus" under extraterritoriality law, the *Charming Betsy* canon *independently* blocks the illegal exercise of enforcement jurisdiction the Government seeks to authorize in this case.

C. The Government's position is irreconcilable with our international legal obligations and *Charming Betsy*.

The Government never mentions *Charming Betsy* by name, even to distinguish it. And it makes no attempt to dispute any of these bedrock principles of international law. Instead, it tries various ways of minimizing the obvious clash between its position on unilateral cross-border searches and these principles of international law and statutory interpretation. None of these efforts is persuasive.

1. No international treaty permits unilateral trans-state seizure of private electronic data.

The closest the Government comes to acknowledging its obligations under international law is its reference the Council of Europe Convention on Cybercrime Nov. 23, 2001, S. Treaty Doc. No. 11, 108th Cong., 1st Sess. (2003), 2296 U.N.T.S. 167 (the Budapest Convention), to which the U.S. and Ireland are both signatories. The Government asserts that the Budapest Convention obliges the U.S. to adopt legislation allowing it to unilaterally seize data located in other countries through production orders aimed at U.S.-based service providers. Then it points to the absence of any implementing legislation enacted after the treaty's ratification as a sign that Congress believed the SCA to already contain that requisite authority. Gov't Br. 47–49.

a. The Convention simply does not do what the Government suggests. The Government contends that the authority for unilateral cross-border searches stems from the Convention's Article 18.1(a), Gov't Br. 48, which allows signatory countries to make provisions for "production order[s]" that their law-enforcement officials may use to compel a person located in the party's territory to turn over data within that person's "possession or control." But nothing in Article 18.1(a) expressly authorizes use of production orders issued in one country to access private data stored in another country, even if within the "possession or control" of a person located in the party's territory.

That dooms the Government's argument. Treaties like the Convention must be "interpreted against the background of the general principles of international

law." Baron Arnold Duncan McNair, *The Law of Treaties* 466 (2d ed. 1961); see also Vienna Convention on the Law of Treaties, May 23, 1969, art. 31.3(c), 1155 U.N.T.S. 331 (requiring that "[a]ny relevant rules of international law applicable in the relations between the parties" be taken into account in interpreting treaties). Those background legal principles strictly prohibit unilateral cross-border seizures. And those restrictions remain in force because they have not been overridden by Article 18's "express terms." Joost Pauwelyn, *The Rule of Public International Law in the WTO: How Far Can We Go?*, 95 Am. J. Int'l L. 535, 541 (2001) (quoting *George Pinson (Fr.)* v. *United Mexican States*, 5 R.I.A.A. 327 (422 Perm. Ct. Arb. 1928)). Interpreting Article 18.1(a) to allow unilateral cross-border data seizures would thus be inconsistent with both the Convention's unambiguous terms and universally accepted principles of treaty interpretation.

b. Interpreting Article 18.1(a) to allow production orders to reach data stored in other countries would also be inconsistent with the Convention's Article 32. That provision, entitled "Trans-border access to stored data," makes clear that the Convention leaves in place virtually all preexisting domestic laws regarding warrant enforcement, and has virtually no effect on parties' obligations under international prohibiting unilateral cross-border data seizures. Article 32 provides that unless a party obtains the authorization of another party, it may only access data stored in another country if that data is "publicly available," or the party obtains the "lawful and voluntary consent" of a person with the "lawful authority to disclose the data"—normally only the data's owner. If the data stored in another country is privately kept, and

the searching party does not obtain consent, Article 32 provides no avenue to unilaterally access it. And the remainder of the Convention does not either. These strict restrictions that permit access to data stored abroad in only exceptionally narrow circumstances—no matter what means of access are employed—cannot be reconciled with the Government's broad view of Article 18, which would allow law-enforcement personnel virtually unimpeded access to data stored in other countries simply because that access is obtained through a production order.

Article 32's strict restrictions on cross-border seizures exist because the Convention's parties could not reach mutually acceptable terms allowing for anything more. As the Convention's Explanatory Report explains, the issue "of when a Party is permitted to unilaterally access computer data stored in another Party without seeking mutual assistance" was "discussed at length" at the convention. Convention on Cybercrime Explanatory Report ¶293 (Nov. 23, 2001). But the drafters "ultimately determined that it was not yet possible to prepare a comprehensive, legally binding regime regulating this area." *Ibid.* The Government's interpretation of the Convention thus requires inserting terms into the treaty concerning matters on which the parties were explicitly unable to reach consensus.

c. It is thus perhaps unsurprising that the Government's only supporting authority comes from a snippet culled from a Guidance Note that was drafted separately from the Convention itself. Gov't Br. 49 (citing Cybercrime Convention Committee, Council of Europe, T-CY Guidance Note #10 (Mar. 1, 2017) (Guidance Note)). Less surprising still is that this slender reed proves in-

adequate to the task. The document, which declares itself to be "not binding," Guidance Note art. 1, provides that production orders may be used to uncover "subscriber information" located in other countries. But this reference to "subscriber information" does not implicate Article 18.1(a), upon which the Government relies. Instead, its reference to "subscriber information" dovetails with the terms of *Article 18.1(b)*, on which the Government does not rely. This is because Article 18.1(b) envisions a different sort of situation, in which a service provider is "offering its services in the territory of the Party," *ibid.*, but is not "necessarily located in the territory," Guidance Note art. 1—for instance, if Microsoft's headquarters were located in Ireland but the company still served the U.S. market. In such circumstances, Article 18.1(b) allows law enforcement officials to obtain "subscriber information" even if it requires obtaining it from the provider's home country. Budapest Convention art. 18.1(b).

Article 18.1(b)'s promise of access to "subscriber data" is also a far cry from the right of untrammeled cross-border access to non-U.S. citizens' private emails that the Government claims. If the Government were to demand that a party turn over "subscriber information," as that term is defined under Article 18.3 of the Convention, it would receive only details about the subscriber's identity, such as her name and address, along with her means of electronic access and the services she consumes. It would not be entitled to obtain the private contents of email communications—because "subscriber information" is defined to *exclude* any such "traffic or content data," which remains private. Budapest Convention art. 18.3. This is consistent with the idea from Article 32 that

such private data is largely shielded from unilateral cross-border access.

As for Article 18.1(a), the Guidance Note envisions that this provision will allow law-enforcement officers to compel a person to disclose his or her *own* information, not private information belonging to third parties. This is confirmed by the Explanatory Report, which anticipates that a production order issued under Article 18.1(a) would be used to seize "information stored in *his or her* [own] account," not the information in some third-party's account. Explanatory Report ¶173.

The Government's expansive interpretation is also at war with other provisions within the Guidance Note. The Guidance Note makes clear that production orders allowed under Article 18 are purely "domestic" in character—"to be provided for under domestic criminal law." Guidance Note art. 3.4. And the power to issue these orders is "constrained by the adjudicative and enforcement jurisdiction of the Party in which the order is granted." *Ibid.* Indeed, the Guidance Note contains a savings clause providing that agreement to the Guidance Note would not constitute "consent to the extraterritorial service or enforcement of a domestic production order issued by another State." *Id.* art. 3.3.[2]

---

[2] The Government will argue that the Guidance Note's reference to "extraterritorial service or enforcement" is meant to address circumstances in which one party—the issuer of a production order—seeks to force *another party*—the one in whose territory the data is located—to seize the data on the issuing party's behalf. But it is unlikely that the Guidance Note would devote time to explicitly addressing such rarely occurring circumstances. The better view is that this passage speaks precisely to the issue in this case—namely,

Further still, the Guidance Note confirms that Article 18.1 was meant to overcome *corporate* legal barriers, not *geographic* ones. It clarifies that "[t]he term 'possession or control' refers to [both] physical possession of the data concerned in the ordering Party's territory," and situations involving "constructive possession," such as when the data is housed by some "remote online storage service." Guidance Note ¶173.

Taken together, these provisions in the Guidance confirm that international law's territorial limits on seizures survived the Convention. Geographically speaking, warrants extend no further after the Convention than they did before. And if parties wish to authorize unilateral trans-state seizures of data, they must instead look outside the Convention—to some law extending enforcement of production orders into other countries, or some other treaty by which countries have mutually agreed to allow the unilateral enforcement of production orders among themselves. While the Guidance raises the abstract possibility that a production order might issue to allow a party to recover data stored overseas, it is clear in context that such unilateral access can only occur if the party's law already allowed for it.

The Government's reliance on the Guidance Note also requires a series of unsustainable chronological and inferential leaps. Nothing indicates that this document, written in 2017, actually captured any signatory's understanding of the Convention when it was enacted more

---

a party's effort to enforce a domestic production order extraterritorially *on its own*, by ordering production of third-party data stored abroad through remote access.

than a decade and a half before in 2001—much less what Congress meant still a decade and a half *before then*, when it enacted the SCA in 1986, Pub. L. No. 99-508, tit. II, 100 Stat. 1860 (Oct. 21, 1986). More fundamentally, these stacked inferences of implied congressional intent lack the express clarity that *Charming Betsy* and the law of extraterritoriality each require before Congress can be understood to have authorized extraterritorial enforcement or sanctioned violations of international law.

d. The Government's view of Article 18's reach is also difficult to square with the Convention's larger goals, which aim to promote cooperation on remote searches through MLAT procedures. The Convention broadly adopts an approach that limits searches to data located in the party's home country as outlined in Article 19—which only provides for authorities to access data "stored in its territory." Article 32 anticipates that when the data is stored in another country, the best route to obtaining it will normally lie through that other party's "consent"—clearly anticipating the existence of an MLAT. This consensus-based framework throws the legal barriers imposed by international law on cross-border searches into high relief. The Government's go-it-alone read of the Convention, by contrast, goes against its consensus-emphasizing grain, and renders the Convention's provisions anticipating party consent—and their implicit references to MLATs—entirely irrelevant. Accordingly, the Convention's text and context both confirm that the Convention never meant to authorize unilateral cross-border searches, and does not reflect any understanding that the SCA does so either.

2. The Government's analogy to civil subpoenas fails.

Equally flawed is the Government's attempt to close the distance between its position and the dictates of international law by analogizing Section 2703 warrants to civil subpoenas of a company's own business records. The Government points to lower court decisions authorizing use of these subpoenas to compel collection of information stored abroad, Gov't Br. 14, 32–34, calling this the "backdrop" against which the SCA was enacted, *id.* at 32. But the subpoena analogy is a bad one for the Government, as it only highlights the perils of the Government's neglect of the *Charming Betsy* canon by illustrating how lower courts have neglected it too.

Subpoenas ordering parties to produce documents or data physically located in other countries may not generally be considered exercises of extraterritorial enforcement jurisdiction, as they are usually issued at the behest of private parties, not government officials. But they are nonetheless viewed by virtually every other country as a violation of national sovereignty. International Law Association, *Report of the Fifty-First Conference* 407 (1965) ("It is difficult to find any authority under international law for the issuance of orders compelling the production of documents from abroad. The documents are admittedly located in the territory of another state."). They are also likely a violation of the international legal principle of nonintervention, which prohibits all acts intended "to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights and to secure from it advantages of any kind." United Nations, General Assembly, Resolution 2625 (XXV), annex, *Declaration on Principles of Inter-*

national Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations (Oct. 24, 1970).

Even if judicially sanctioned international incursions via subpoena were not violations of international law, they would still offend "comity"—"the respect sovereign nations afford each other by limiting the reach of their laws." *Hartford Fire*, 509 U.S. at 817 (Scalia, J., dissenting). "That comity is exercised by legislatures when they enact laws," and courts likewise "*assume* it has been exercised" when executing their judicial functions. *Ibid.* (citing J. Story, *Commentaries on the Conflict of Laws* § 38 (1834), emphasis added).

Comity is as binding on courts as statutory law. As Justice Cardozo explained while still on the New York Court of Appeals in *Loucks* v. *Standard Oil Co. of New York*, "[t]he misleading word 'comity' has been responsible for much *** trouble" by suggesting, wrongly, that courts have discretion to disregard international comity. 224 N.Y. 99, 111 (1918). To the contrary, only the Legislature possesses such discretion. But Congress has done nothing to extend the civil subpoena power internationally. Nothing suggests Congress *would* sanction such power either, because of the pronounced friction the U.S.'s international discovery practices have provoked. "No aspect of the extension of the American legal system beyond the territorial frontier of the United States has given rise to so much friction" as broad U.S. discovery in international cases. *Restatement (Third) of the Foreign Relations Law of the United States* § 442, Reporters' Note 1 (1987). This is not just abstract theorizing. Foreign nations and the European Commission itself have written to express their view that our civil data-collection

efforts are akin to foreign invasion: "a territorial encroachment without justification, one which is exacerbated by the sharp differences in the legal status of personal data in the U.S. and EU." Albrecht C.A. Amicus Br. 10; see also Ireland C.A. Amicus Br. 7.

Some countries have gone so far as to enact blocking statutes in direct response to U.S. courts' exorbitant discovery practices, Gary B. Born & Peter B. Rutledge, *International Civil Litigation in U.S. Courts* 969–978 (5th ed. 2011). One such statute, Article 1A of French Penal Code Law No. 80-538, expressly prohibits turning over information absent a treaty or other international agreement, an obvious manifestation "of French displeasure with American pre-trial discovery procedures." *Graco, Inc.* v. *Kremlin, Inc.*, 101 F.R.D. 503, 508 (N.D. Ill. 1984). And when the European Union's General Data Protection Regulation (GDPR) goes into effect in May, it will pose further barriers to enforcement of civil subpoenas abroad, generally refusing to permit enforcement of a "judgment of a court *** requiring a [provider] to transfer or disclose personal data" unless the order is "based on an international agreement." Commission Regulation 2016/679, art. 48, 2016 O.J. (L 119) 64. While the European Commission explains in its brief that there are derogations in the GDPR that could in some cases allow compliance with a unilateral U.S. warrant, those derogations are limited and apply only on a case-by-case basis. Indeed, just two weeks ago, the French Government issued a statement declaring that the Government's position in this case risked a significant conflict with the GDPR. *États-Unis – Union européenne - Q&R - Extrait du point de presse* (Jan. 4, 2018), <https://goo.gl/ferJG8>. These strong international re-

actions demonstrate that when it comes to international discovery and evidence gathering, the United States is resented as an outlier.

Charming Betsy's insight stems from the recognition that Congress is cognizant of these potential foreign-affairs flare-ups, and normally seeks to avoid them, not stoke them. That assumption is only reinforced through the Senate's ratification of MLATs whose whole reason for being is to respect the sovereignties of other countries and smooth international friction by setting terms under which the gathering of evidence abroad can be done consensually. To take Congress's silence regarding international enforcement of civil subpoenas as approval of these internationally condemned practices flies in the face of *Charming Betsy* and its insights about Congress's approach to lawmaking. The subpoena analogy is therefore poor ground for the Government to build its case upon.

To stress this unsound foundation still further, and enlarge this projection of U.S. power into the area of Section 2703 warrants is far worse, because warrants are much more significant intrusions nations' sovereignty and the liberties of their citizens than subpoenas. Unlike civil subpoenas, warrants are a tool of criminal law enforcement. And unlike subpoenas, they are not restricted to searches of property belonging to companies that are subject to the jurisdiction of U.S. courts—implying that the subject of the subpoena has *some* U.S. connection. If the Government is correct, Section 2703 warrants would allow seizures of data from anywhere in the world, and because providers often keep such data near their customers, Resp. Br. 7, that effectively empowers U.S. officials to investigate *any* foreign citizen. Allowing that re-

sult will only produce additional friction. It will also likely invite retaliation from other countries that will be tempted to seize our citizens' data through providers like Microsoft located in their territories, and would likely do so without bothering to respecting our citizens' constitutional rights, which limit the power of *our* government, not theirs.

In short, reading the Stored Communications Act in a way that reaches foreign-stored data guarantees the very clash with international law *Charming Betsy* sought to avoid. If Congress wishes to authorize such broad, unilateral law enforcement powers instead of engaging in cooperative treaty solutions, so be it. But Congress gets to make that decision. For courts to insert themselves into these sensitive and important foreign policy decisions is inappropriate. This Court should decline the Government's invitation to do so.

II. Transnational seizures of private electronic data also exceed the SCA's territorial boundaries.

The Government's analysis of the law of extraterritoriality does not disregard the doctrine outright—as it does with *Charming Betsy*. But it still refuses to fully engage in the "focus" analysis this Court demands to ensure purely domestic laws remain domestic, and are not applied extraterritorially. *RJR Nabisco, Inc.*, 136 S. Ct. 2010. The Government frames the SCA's warrant provisions as focused only on "disclosure," solely because Section 2703 uses the term "disclosure." And because the Government sees "disclosure" as occurring only in the United States, that legerdemain allows the Government to free itself from the SCA's acknowledged territorial boundaries, authorizing it—along with state and local law-enforcement officials—to physically seize data from

anywhere in the world. But the Government misunderstands the focus analysis, and its narrow conception of Section 2703's focus is unsupportable. Even if the Government is right that Section 2703's focus is restricted to disclosure, seizing foreign citizens' private emails located in foreign countries still cannot be ignored as the inconsequential byproduct of that disclosure.

A. The Government's effort to sanction the unilateral seizure of private emails of foreign citizens stored abroad impermissibly narrows the focus inquiry.

The flaws in the Government's focus analysis begin with its failure to recognize that the SCA is a product of its time. When Congress enacted the SCA in 1986, it did not "intend that the Act regulate activities conducted outside the territorial United States." H.R. Rep. No. 99-647, at 32–33 (1986). Its provisions regarding access to stored wire and electronic communications were "intended to apply only to access within the territorial States." *Ibid.* Back then, the ability to transmit and store electronic information abroad—a seamless process in today's world of non-localized "cloud computing"—did not even exist. Pet. App. 14a. And federal criminal law-enforcement was considered largely a domestic, rather than international, affair. *See* National Commission of Reform of Federal Criminal Laws, *Final Report* 21 (1971) ("[T]he issue of extraterritorial application of the federal criminal law is one which does not arise frequently."). From this historical perspective, it must be assumed that Congress anticipated the SCA to apply only to the domestic storage of data—and purely domestic disclosures of data. Indeed, that is the only explanation for Congress's decision to allow state and local law enforce-

ment to use the SCA. Congress could never have conceived of, let alone authorized, retrievals of communications stored in foreign countries.

The Government's effort to prove otherwise strips Section 2703 of this larger historical context. At best, this effort is merely a guess about what Congress's focus *would* have been, and the laws Congress *would* have enacted, if it could have anticipated the technological changes that would occur a generation later with the globalization of data—exactly the sort of "speculation" and "divining what Congress would have wanted" that the Court properly prohibits. *Morrison*, 561 U.S. at 261. At worst, the Government's position is a transparent attempt to change the focus analysis's basic purpose, and unnaturally restrict the scope of conduct that might be deemed extraterritorial, simply so that it might evade the SCA's domestic limits. But the focus analysis *reinforced* the territorial boundaries of purely domestic laws; it provides no means to evade them. Indeed, just as *Morrison* demonstrates that the law of extraterritorially does not lose its bite simply upon encountering *some* domestic conduct, it surely is not so craven as to flinch before such transparent efforts to nullify the presumption.

The Government's narrow view of what "disclosure" entails presents separate problems. Disclosure cannot be understood as solely the act of turning data over to the government viewed in isolation. Disclosure involves a whole series of steps—including the retrieval of the underlying data from storage—that must be performed to effectuate the disclosure. Law-enforcement officials' authority to compel these actions comes exclusively from the SCA. Accordingly, that entire range of conduct is

properly viewed as within Congress's "focus," and is thus subject to the SCA's acknowledged domestic limits.

The Government's contrary view that "disclosure" refers only to the isolated act of turning data over to the government, simply because the term actually appears on the page in Section 2703, Gov't Br. 22–23, is ultimately grounded on the focus analysis conducted in cases like *Morrison* and *RJR Nabisco*, Gov't Br. 19–20. Certainly both of those cases restricted their analysis to the language of specific statutory provisions. *RJR Nabisco*, 136 S. Ct. 2101–2103; *Morrison*, 561 U.S. at 262–265. And the narrow, text-focused inquiry employed in *Morrison* and *RJR Nabisco* was not only permissible for the statutes at issue in those cases, but necessary to protect their territorial limits. Such statutes subject private parties to liability, and may involve factual scenarios involving actors and conduct occurring in a variety of countries. Confining the focus of such statutes to their specific terms is essential to ensure that their territorial boundaries are respected, and that foreign nations, and foreign transactions, are not subjected to liability without congressional approval.

That said, there are clues right in the SCA's text that Congress views "disclosure" entailing more than simply turning data over to the government. The Act recognizes that disclosure involves all the steps needed to compel the "execution of a search warrant" by the provider on the Government's behalf, 18 U.S.C. § 2703(g), including the retrieval of the underlying data from "electronic storage," *id.* § 2703(a).

But even if these textual clues were absent, an examination of the SCA's focus must consider the entire realm of conduct it authorizes. This is because the analysis re-

quired for domestic statutes like the SCA, which convey power to public government officials, is necessarily more searching than a simple examination of the text, requiring instead a consideration of the *context* in which that power will be exercised. And when a domestic statute authorizes governmental actors to undertake a particular sequence of conduct, the entire sequence of authorized conduct must be understood as within the statute's focus, and confined to the statute's territorial limits, even when some of that authority is necessarily implied.

So it was in *Kiobel* v. *Royal Dutch Petroleum Co.*, 569 U.S. 108 (2013). There the Court was tasked with deciding whether the Alien Tort Statute (ATS), 28 U.S.C. § 1350, a law with no "extraterritorial reach," *Kiobel*, 569 U.S. at 118, authorizes causes of action for violations of the law of nations occurring entirely within the territory of a foreign sovereign. That question could not be resolved from the ATS's text alone, because the ATS is "strictly jurisdictional," *Kiobel*, 166 U.S. at 116 (quoting *Sosa* v. *Alvarez–Machain*, 542 U.S. 692, 713 (2004)), conveying power to district courts to entertain claims. It does not "expressly provide *any* causes of action." *Kiobel*, 569 U.S. at 115 (emphasis added). The Act is silent about whether it covered violations of the law of nations occurring abroad.

Thus, the Court explained, a different kind of analysis was necessary from cases like *Morrison*, which involved a statute "regulating conduct," *Kiobel*, 569 U.S. at 116 (citing *Aramco*, 499 U.S. at 246, not one concerning "a question of jurisdiction" conveyed to a court. *Ibid.* (citing *Morrison*, 561 U.S. at 254). And, the Court explained, that difference demanded that it go well beyond deciding "what Congress has done" in the ATS itself,

ibid., since Congress did not address extraterritorial claims specifically. Rather, it required determining what "courts may do" with the authority Congress had conveyed to them through the jurisdiction provided by the ATS, *ibid.* The Court thus looked to the full range of "what courts may do" in applying the ATS to determine whether it was being applied extraterritorially—whether those things were specifically enumerated in the statute or not.

Kiobel's approach translates exactly to this case. Determining whether law-enforcement may undertake cross-border seizures under a Section 2703 warrant is less a question of what Congress itself has done—in the precise language of the statute—to regulate such searches, but what it *authorizes* those law-enforcement officials to do in the real world, and whether law-enforcement officials have exercised that authority in a manner that exceeds the SCA's territorial boundaries. And that broader, functional view of Congress's focus is essential to ensure that government officials do not exceed the statutory authority Congress has conveyed to them. When, as here, a portion of that authorized conduct occurs abroad, it exceeds the power conveyed by Congress.

B. The principles that drive extraterritoriality analysis support this broad reading of Section 2703's focus.

That conclusion is only reinforced by the principles underlying the extraterritorially analysis. These principles "constrain courts," *Kiobel*, 569 U.S. at 116, and ought to inform determinations of about the "focus" of

domestic statutes like the SCA just as they inform determinations about whether those statutes *are* domestic.

Those principles powerfully counsel in favor of taking a broad view of the SCA's applicable focus in this case, to incorporate all conduct authorized in effectuating "disclosure." That result will best avoid friction with other countries—and clashes between our laws and theirs—and it will protect Congress's prerogatives in lawmaking, so that domestic statutes like the SCA do not slip their territorial boundaries through extraterritorial application.

1. The Government's approach invites clashes with foreign nations without congressional authorization.

The Court strains to avoid interpretations of "U.S. law that carr[y] foreign policy consequences not clearly intended" by Congress. *Kiobel*, 569 U.S. at 116. And it is wary of interpreting statutes in ways that avoid producing "friction" with foreign countries, *RJR Nabisco*, 136 S. Ct. at 2106–2108. But the Government's reading of the SCA introduces just these kinds of unintended foreign-policy consequences and friction with other nations. Issues concerning the handling of foreign citizens' personal data, and conducting law-enforcement actions abroad, will naturally arouse the suspicion of foreign sovereigns. Those issues arise here in an international environment already inflamed by this country's aggressive stance on civil discovery. To feed those flames by extending that stance into the far more intrusive criminal context is a terrible idea. And allowing the Government to implement this policy without being forced to make its case to Congress why such intrusion is necessary will invite abuse and overreach, especially when the targets of

these law-enforcement activities will virtually always be foreign nationals who lack strong voices in our national government. That incentive toward overreach will in turn increase the risk of retaliation, potentially fostering an ever-escalating conflict. Consideration of these "adverse foreign policy consequences" should leave the Court reluctant to rule in the Government's favor. *Kiobel*, 569 U.S. at 124 (quoting *Sosa*, 542 U.S. at 727–728).

Extending our warrant power to collect data stored abroad—thereby imposing our laws regarding the collection of data in other countries—will also produce direct clashes with other countries' legal regimes. By law and by treaty, other countries have different rules for protecting digital property, and different rules for court-compelled disclosure of information. Anthony J. Colangelo, *Absolute Conflicts of Law*, 91 Ind. L. J. 719, 734–735 (2016). In many such situations, compliance with one law will invariably lead to violation of the other. *Ibid.* (describing "procedural absolute conflicts of law" where "one state's litigation-oriented discovery order compels production of information and another state's litigation-oriented law prevents the production of that information"). That could put many American electronic service providers like Microsoft in impossible situations, with potentially criminal consequences, when they do business abroad. And the only assurance that the Government offers to assuage these concerns—that such clashes have not happened *yet*—offers cold comfort, and contradicts concerns that Government itself has raised in other forums. *Law Enforcement Access to Data Stored Across Borders: Hearing Before the S. Subcomm. on Crime and Terrorism* (May 24, 2017), at 50:30–51:40, <goo.gl/T7Ai7u> (testimony of Brad Wiegmann, Deputy

Assistant Att'y Gen., U.S. Dep't of Justice) (stating that "when U.S. authorities are seeking data overseas," there is always least the "potential for conflicts"). Such potential regulatory nightmares strongly indicate that "if Congress intended such foreign application 'it would have addressed the subject of conflicts with foreign laws and procedures'" itself, *Morrison*, 561 U.S. at 269 (quoting *Aramco*, 499 U.S. at 256).

Finally, if history is any guide, a ruling for the Government that sanctions unilateral international seizures under Section 2703 could have real-world consequences for ongoing international efforts to address these pressing issues and bring harmony to this area of international law, "a matter of increasing importance in an ever more interdependent world." *Sosa*, 542 U.S. at 761 (2004) (Breyer, J., concurring). In the past, when courts have rejected government arguments for extending domestic statutes extraterritorially, those refusals have served as encouragement for the U.S. to engage in bilateral or multilateral efforts to overcome these limitations. See Tonya Putnam, *Courts Without Borders* 6 (2016). A ruling for the Government will diminish any incentive for the U.S. to come to the bargaining table, and undermine the international forces working toward harmony.

2. The Government's approach undermines the separation of powers and shared assumptions about Congress's approach to lawmaking.

Adopting the Government's wooden approach to extraterritoriality, and its narrow position on the SCA's focus, will also put serious strain on the separation of powers, in ways that Congress is presumed to avoid in enacting statutes. Requiring courts to authorize Section 2703

warrants allowing for the seizure of data physically located in other countries would force them into disputes with other countries on extraordinarily sensitive foreign-affairs issues. It would be odd indeed for Congress to assign these issues to federal district courts, especially without equipping them with mechanisms to reduce that friction.

And courts should not assume those responsibilities for themselves. These foreign-affairs issues properly belong to Congress, the branch that possesses the constitutional authority to address foreign policy in lawmaking, which alone has the institutional capacity to craft the nuanced policies needed to navigate such dangerous waters. For courts to step in and bless unilateral executive action would displace Congress's proper role. And it would disrupt the constitutionally mandated conversation between Congress and the Executive over how these issues ought to be handled, diminishing any incentive for the branches to engage in the heavy lifting needed to craft appropriate international and domestic policy solutions.

Congress likewise would never have allowed state and local officials to insert themselves into these delicate foreign-affairs issues. They are among the "governmental entities" that Congress permits to use Section 2703's warrant provision. 18 U.S.C. § 2711(4). But they lack the competence, constitutional authority, and political accountability to our national polity that Congress would certainly have demanded of anyone it had chosen to assume such sensitive duties.

The cacophony of different voices introduced under the Government's interpretation also undermines the principle that the government must speak with "one

voice" in foreign affairs. *Japan Line, Ltd.* v. *Cty. of Los Angeles*, 441 U.S. 434, 449 (1979). And it risks "impinging on the discretion of the Legislative and Executive Branches in managing foreign affairs." *Kiobal*, 569 U.S. at 116 (internal quotation omitted). How could Congress promise to engage in consensual processes for handling data in negotiations with other countries, while at the same time authorizing other actors—those over which it has no direct control—to proceed unilaterally? More importantly, why would Congress ever put itself into that untenable position in the first place? The Government cannot answer these concerns.

Further, the Government's narrow approach to extraterritoriality also depends upon the idea that electronic incursions ought to count less—or not count at all—in the focus analysis. That seed should be allowed no room to spread, as it would undermine the basic bargain between Congress and the Court about how the laws Congress enacts will be applied over time. When Congress enacts laws, it makes use of the Court's cautious approach to extraterritoriality, and counts on the courts to maintain a consistent application of those doctrines over time. That allows Congress to legislate with confidence that those doctrines will protect the territorial limits of its laws, so unforeseen circumstances do not create unintended international implications for purely domestic laws. Indeed, the enactment of the SCA is a perfect illustration of this phenomenon. The Court's extraterritorially doctrines are thus a hedge *against* the march of technological change and the expansion of global information networks, meant to halt extraterritorial creep at the border. They should not be interpreted to facilitate it.

If the Government's approach to extraterritoriality became the law, it would mean that as the world changes and becomes even more globalized, Congress will have to periodically revise its own domestic laws simply to ensure that they *remain* domestic, and must devote resources to anticipating and monitoring extraterritorial creep. That reverses the presumption against extraterritoriality, and forces Congress to do the work that it rightly counts on extraterritorial doctrine to do for it. For all these reasons, the Government's narrow view of the extraterritoriality analysis ought to be rejected.

C. The Government's concerns about protecting law-enforcement efficacy are best addressed to Congress.

The Government raises concerns that enforcing Section 2703's domestic limits will hamper law enforcement. It worries that making the ability to obtain evidence in criminal investigations turn upon a "provider's business decision" might invite abuse, Gov't Br. 42. It also raises concerns that MLATs cannot provide a "reliable substitute" for a Section 2703 warrant because too few such treaties exist, and proceeding through them can be a slow, cumbersome, and uncertain process. *Id.* at 44.

Amici do not mean to minimize these concerns, but they are addressed to the wrong body. The Government provides nothing to suggest that Microsoft or any other provider moves data to deliberately interfere with legitimate law-enforcement objectives. Congress would certainly care if any provider did engage in such shenanigans. And if Section 2703 does not currently meet law enforcement needs, and unilateral seizures are truly necessary to properly investigate transnational crimes,

then the Government should explain to Congress why the statute ought to be amended. That would provide Congress its rightful opportunity to weigh the need for such reforms against the international friction they would inevitably foster. As Microsoft explains, this process is already ongoing, and Congress has given every indication that it will take the Government's legitimate concerns into account. Likewise, if MLATs do not yet provide a workable alternative, that should only spur the U.S. to further engage internationally, so that it might create more effective treaty solutions—and more of them—and to develop international standards that will address these difficult transnational problems as the world changes.

* * *

In a rapidly shrinking world, dramatic changes related to transnational crime and data challenge traditional understandings about territorial regulation. The Government may ultimately convince Congress that the policy reasons supporting its position are stronger than the policy reasons supporting Microsoft's. But these complicated policy issues implicate important principles of international law. Both the *Charming Betsy* canon and the law of extraterritoriality require that in such instances the Court not act, but allow Congress to act first. Pushing the Executive to engage with Congress is the right result.

CONCLUSION

The judgment of the court of appeals should be affirmed.

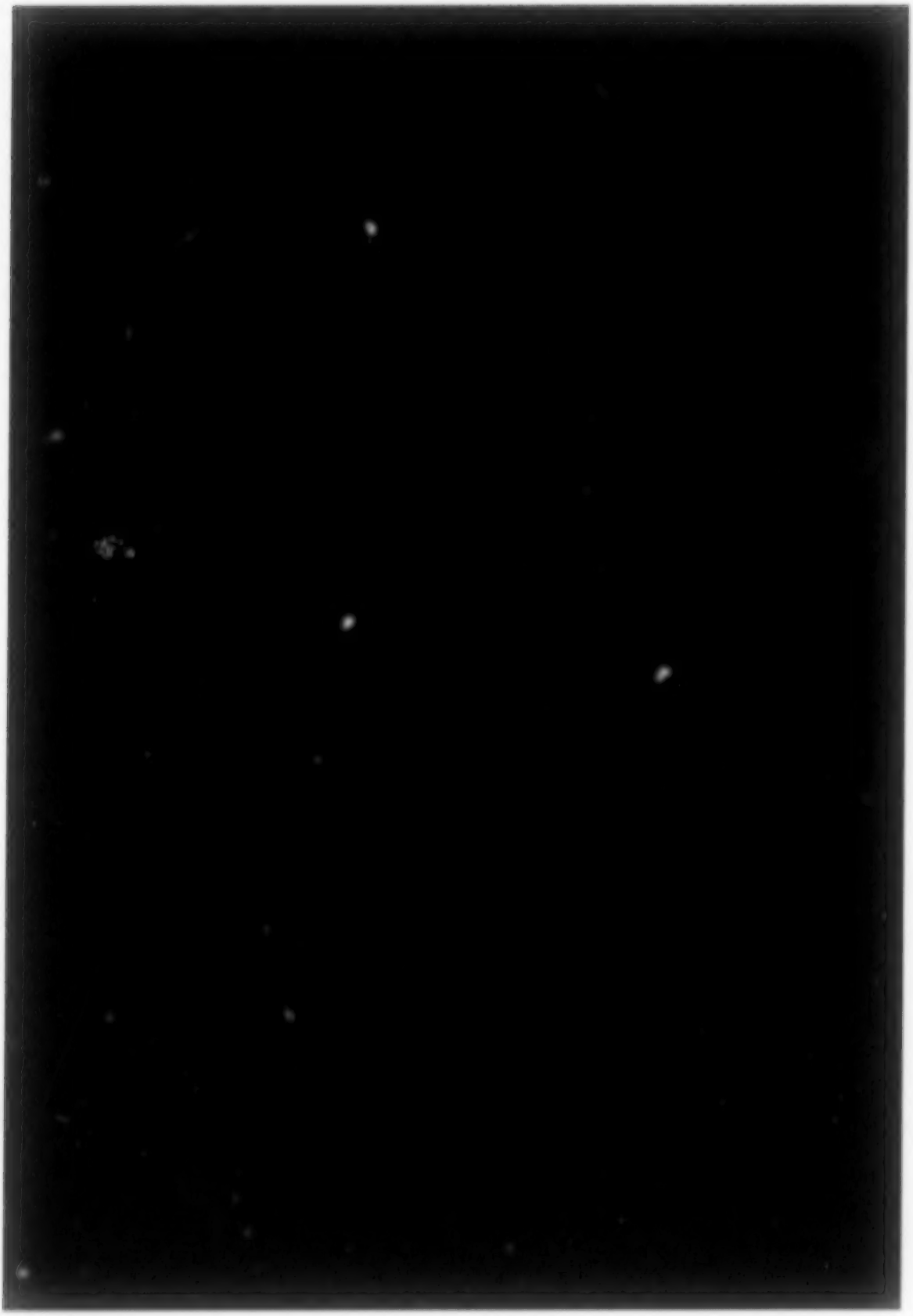
Respectfully submitted,

Anthony Colangelo
SMU DEDMAN SCHOOL OF LAW
3315 Daniel Ave.
Dallas, Texas 75205
(214) 768-2372

J. Carl Cecere
Counsel of Record
CECERE PC
6035 McCommas Blvd.
Dallas, Texas 75206
(469) 600-9455
ccecere@cecerepc.com

Austen Parrish
IU MAURER SCHOOL OF LAW
211 S. Indiana Ave.,
Bloomington, Indiana 47405
(812) 855-8885

January 18, 2018



INDEX

Appendix..... 1a

APPENDIX

Cassandra Burke Robertson – Professor Burke Robertson is the John Deaver Drinko - BakerHostetler Professor of Law and Director of the Center for Professional Ethics at Case Western Reserve University School of Law. She serves as one of Ohio's representatives to the Uniform Law Commission (also known as the National Conference of Commissioners on Uniform State Laws) and chairs the Appellate Litigation subcommittee of the American Bar Association's Civil Rights Litigation Committee. Professor Robertson teaches Civil Procedure, Professional Responsibility, and Transnational Litigation. Her scholarship focuses on legal ethics and litigation procedure within a globalizing practice of law. She has co-authored a popular casebook in the field of professional responsibility. Her articles on transnational litigation and procedure have appeared in the Columbia Law Review, Emory Law Journal and Boston College Law Review, among others.

Anthony J. Colangelo – Professor Colangelo is the Gerald J. Ford Research Fellow and Professor of Law at the SMU Dedman School of Law. He specializes in the areas of extraterritorial jurisdiction and international law. Representative articles include, *A Unified Approach to Extraterritoriality* in the Virginia Law Review and *What Is Extraterritoriality?* In the Cornell Law Review.

Austen L. Parrish – Dean Parrish is the Dean and James H. Rudy Professor at Indiana University Bloomington Maurer School of Law. He has taught

courses in civil procedure, federal courts, public international law, international environmental law, and transnational law. For seven years, he directed a summer international and comparative law program at the University of British Columbia in Vancouver, B.C., Canada, hosted in collaboration with the International Centre for Criminal Law Reform and Criminal Justice Policy. He has written a number of articles focused on private international and cross-border litigation, international law, and extraterritorial jurisdiction. Prior to entering academia, he worked in private practice focused on complex civil litigation with O'Melveny & Myers LLP.

Tonya Lee Putnam – Professor Putnam is Associate Professor of Political Science at Columbia University. Professor Putnam is also a graduate of Harvard Law School and member of the California State Bar. Her research engages themes at the intersection of international relations and international law, including jurisdiction and extraterritoriality, international and transnational regulation, human rights, international humanitarian law, migration, institutional design, and judicial politics. She is the author of *Courts Without Borders: Law, Politics, and U.S. Extraterritoriality* (Cambridge University Press 2016) and several peer-reviewed articles. In 1998-1999, Professor Putnam also served as a member of Namibia's legal counsel in the *Kasikili/Sedudu Island (Botswana v. Namibia)* at the International Court of Justice.

Robert D. Sloane – Professor Sloane is the R. Gordon Butler Scholar in International Law at Boston University Law School. He is an elected member of the American Law Institute and serves on the Members Consultative

Group for the Restatement (Fourth) of Foreign Relations Law. In 2013. Professor Sloane's scholarship focuses on international law and related fields including national security and foreign relations law, the law of war, international criminal law, jurisprudence, and international dispute resolution.

Daniel J. Solove – Professor Solove is the John Marshall Harlan Research Professor of Law at the George Washington University Law School. He is also the founder of TeachPrivacy, a company that provides privacy and data security training programs to businesses, law firms, healthcare institutions, schools, and other organizations.

One of the world's leading experts in privacy law, Solove is the author of numerous books, including *Nothing to Hide: The False Tradeoff Between Privacy and Security* (Yale 2011), *Privacy Law Fundamentals* (IAPP 2011) (with Paul Schwartz), *Understanding Privacy* (Harvard 2008), and *The Future of Reputation: Gossip and Rumor in the Information Age* (Yale 2007). Additionally, he is also the author of several textbooks, including *Information Privacy Law*; as well as more than 50 articles, which have appeared in the *Harvard Law Review*; *Yale Law Journal*, *Stanford Law Review*; *Columbia Law Review*; and many publications. Solove has testified before Congress and has consulted in a number of high-profile privacy cases. He has been featured and interviewed in hundreds of media broadcasts and articles.